REMARKS

By this amendment, Claims 49-52, 54-58, 60-64 and 66 have been amended. Hence, Claims 1-66 are pending in the application. It is respectfully submitted that these amendments do not add any new matter to this application.

The Examiner is invited to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

If there are any additional charges, please charge them to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: October 2, 2001

Edward A. Becker
Reg. No. 37,777

1600 Willow Street
San Jose, California 95125-5106
Telephone: (408) 414-1204
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Washington, DC 20231

on October 2, 2001 by Sheila Severinghaus

CLAIMS IN "MARKED UP" FORM

1. (NOT AMENDED) A method for controlling and tracking access to a message that is communicated from a first node to a second node in a network, the method comprising the computer-implemented steps of:

receiving a request from the first node for a message identifier that uniquely identifies the message and a key that may be used to encode the message;

generating, in response to the request, both the message identifier and the key;

providing both the message identifier and the key to the first node to allow the message to be encoded with the key to generate an encoded message;

receiving a request from the second node for the key;

generating algorithm identification data that indicates an algorithm to be used to decode the encoded message;

providing the algorithm identification data to the second node;

providing the key and the identification data to the second node to allow the encoded message to be decoded and the message to be retrieved using the key; and

deleting the key based upon specified key policy criteria to prevent copies of the encoded message from being decoded.

2. (NOT AMENDED) The method as recited in Claim 1, further comprising:

receiving a second request from the first node for a second message identifier that uniquely identifies a second message and a second key that may be used to encode the second message;

generating, in response to the second request, both the second message identifier and the second key;

providing both the second message identifier and the second key to the first node to allow the second message to be encoded with the second key to generate a second encoded message;

receiving a second request from the second node for the second key;

generating second algorithm identification data that indicates a second algorithm to be used to decode the second encoded message;

providing the second algorithm identification data to the second node;

providing the second key and the second identification data to the second node to allow the second encoded message to be decoded and the second message to be retrieved using the second key; and

deleting the second key based upon the specified key policy criteria to prevent copies of the second encoded message from being decoded.

3. (NOT AMENDED) The method as recited in Claim 1, wherein the decoding identification data further indicates a location wherein the algorithm can be found.

4. (NOT AMENDED) The method as recited in Claim 1, wherein the algorithm identification data is generated at the first node.

5. (NOT AMENDED) The method as recited in Claim 1, wherein the algorithm identification data is stored at a key repository.

6. (NOT AMENDED) A computer-readable medium carrying one or more sequences of one or more instructions for controlling and tracking access to a message that is communicated from a first node to a second node in a network, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving a request from the first node for a message identifier that uniquely identifies the message and a key that may be used to encode the message;

generating, in response to the request, both the message identifier and the key;

providing both the message identifier and the key to the first node to allow the message to be encoded with the key to generate an encoded message;

receiving a request from the second node for the key;

generating algorithm identification data that indicates an algorithm to be used to decode the encoded message;

providing the algorithm identification data to the second node;

providing the key and the identification data to the second node to allow the encoded message to be decoded and the message to be retrieved using the key; and

deleting the key based upon specified key policy criteria to prevent copies of the encoded message from being decoded.

7. (NOT AMENDED) The computer-readable medium as recited in Claim 6, wherein the one or more sequences of one or more instructions include one or more additional sequences of one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

receiving a second request from the first node for a second message identifier that uniquely identifies a second message and a second key that may be used to encode the second message;

generating, in response to the second request, both the second message identifier and the second key;

providing both the second message identifier and the second key to the first node to allow the second message to be encoded with the second key to generate a second encoded message;

receiving a second request from the second node for the second key;

generating second algorithm identification data that indicates a second algorithm to be used to decode the second encoded message;

providing the second algorithm identification data to the second node;

providing the second key and the second identification data to the second node to allow the second encoded message to be decoded and the second message to be retrieved using the second key; and

deleting the second key based upon the specified key policy criteria to prevent copies of the second encoded message from being decoded.

8. (NOT AMENDED) The computer-readable medium as recited in Claim 6, wherein the decoding identification data further indicates a location wherein the algorithm can be found.

9. (NOT AMENDED) The computer-readable medium as recited in Claim 6, wherein the algorithm identification data is generated at the first node.

10. (NOT AMENDED) The computer-readable medium as recited in Claim 6, wherein the algorithm identification data is stored at a key repository.

11. (NOT AMENDED) A computer system for controlling and tracking access to a message that is communicated from a first node to a second node in a network comprising:

one or more processors; and

a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the

one or more processors, cause the one or more processors to perform the steps of:

receiving a second request from the first node for a second message identifier that uniquely identifies a second message and a second key that may be used to encode the second message;

generating, in response to the second request, both the second message identifier and the second key;

providing both the second message identifier and the second key to the first node to allow the second message to be encoded with the second key to generate a second encoded message;

receiving a second request from the second node for the second key;

generating second algorithm identification data that indicates a second algorithm to be used to decode the second encoded message;

providing the second algorithm identification data to the second node;

providing the second key and the second identification data to the second node to allow the second encoded message to be decoded and the second message to be retrieved using the second key; and

deleting the second key based upon the specified key policy criteria to prevent copies of the second encoded message from being decoded.

12. (NOT AMENDED) The computer system as recited in Claim 11, wherein the memory further includes one or more additional sequences of one or more instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

receiving a second request from the first node for a second message identifier that uniquely identifies a second message and a second key that may be used to encode the second message;

generating, in response to the second request, both the second message identifier and the second key;

providing both the second message identifier and the second key to the first node to allow the second message to be encoded with the second key to generate a second encoded message;

receiving a second request from the second node for the second key;

generating second algorithm identification data that indicates a second algorithm to be used to decode the second encoded message;

providing the second algorithm identification data to the second node;

providing the second key and the second identification data to the second node to allow the second encoded message to be decoded and the second message to be retrieved using the second key; and

deleting the second key based upon the specified key policy criteria to prevent copies of the second encoded message from being decoded.

13. (NOT AMENDED) The computer system as recited in Claim 11, wherein the decoding identification data further indicates a location wherein the algorithm can be found.

14. (NOT AMENDED) The computer system as recited in Claim 11, wherein the algorithm identification data is generated at the first node.

15. (NOT AMENDED) The computer system as recited in Claim 11, wherein the algorithm identification data is stored at a key repository.

16. (NOT AMENDED) A method for controlling access to a message that is communicated from a first node to a second node in a network, the method comprising the computer-implemented steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain the encoded message and instructions for decoding the encoded message using the key; and

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message contained in the set of one or more instructions by:

retrieving the key, and

decoding the encoded message using the key.

17. (NOT AMENDED) The method as recited in Claim 16, further comprising deleting the retrieved key.

18. (NOT AMENDED) The method as recited in Claim 16, wherein the set of one or more instructions comprises a set of Javascript instructions.

19. (NOT AMENDED) The method as recited in Claim 16, wherein the set of one or more instructions comprises a set of Java applet instructions.

20. (NOT AMENDED) The method as recited in Claim 16, wherein the set of one or more instructions includes address data that indicates a location from which the key may be retrieved.

21. (NOT AMENDED) A computer-readable medium for controlling access to a message that is communicated from a first node to a second node in a network, the computer-readable medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain the encoded message and instructions for decoding the encoded message using the key; and

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message contained in the set of one or more instructions by:

retrieving the key, and

decoding the encoded message using the key to recover the original message.

22. (NOT AMENDED) The computer-readable medium as recited in Claim 21, further carrying one or more additional sequences of one or instructions which, when executed by the one or more processors, causes the one or more processors to perform the additional step of deleting the retrieved key.

23. (NOT AMENDED) The computer-readable medium as recited in Claim 21, wherein the set of one or more instructions comprises a set of Javascript instructions.

24. (NOT AMENDED) The computer-readable medium as recited in Claim 21, wherein the set of one or more instructions comprises a set of Java applet instructions.

25. (NOT AMENDED) The computer-readable medium as recited in Claim 21, wherein the set of one or more instructions include address data that indicates a location from which the key may be retrieved.

26. (NOT AMENDED) A computer system comprising:

one or more processors; and

a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of::

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain the encoded message and instructions for decoding the encoded message using the key; and

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message contained in the set of one or more instructions by:

retrieving the key, and

decoding the encoded message using the key to recover the original message.

27. (NOT AMENDED) The computer system as recited in Claim 26, wherein the memory further carries one or more additional sequences of one or instructions which, when executed by the one or more processors, causes the one or more processors to perform the additional step of deleting the retrieved key.

28. (NOT AMENDED) The computer system as recited in Claim 26, wherein the set of one or more instructions comprises a set of Javascript instructions.

29. (NOT AMENDED) The computer system as recited in Claim 26, wherein the set of one or more instructions comprises a set of Java applet instructions.

30. (NOT AMENDED) The computer system as recited in Claim 26, wherein the set of one or more instructions include address data that indicates a location from which the key may be retrieved.

31. (NOT AMENDED) A method for controlling access to a message that is communicated from a first node to a second node in a network, the method comprising the computer-implemented steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key ;

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node; and

wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes:

the message to be recovered from the encoded message by

retrieving the key, and

decoding the encoded message using the key, and

the recovered message to be provided from the third node to the second node.

32. (NOT AMENDED) The method as recited in Claim 31, wherein the receiving, at the third node, of the encoded message and the instructions for retrieving the key, further causes the key to be deleted from the third node after the encoded message is decoded.

33. (NOT AMENDED) The method as recited in Claim 31, wherein the set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key comprises an HTML document.

34. (NOT AMENDED) The method as recited in Claim 33, wherein the HTML document comprises an HTML form with fields containing the encoded message and key address data, a submit button to submit the form to the third node, and JavaScript to automatically submit the form to the third node.

35. (NOT AMENDED) The method as recited in Claim 33, wherein the HTML document comprises a set of associated URLs embedded in multiple <img>, <ilayer>, <applet>, or <iframe> elements, wherein each URL contains fragments of the encoded message and key address data as URL query parameters, and wherein each URL specifies the location of the third node.

36. (NOT AMENDED) The method as recited in Claim 35, wherein the URL query parameters also contain control information, which specifies the order and number of message fragments, and enables the third node to reconstruct the complete message.

37. (NOT AMENDED) A computer-readable medium for controlling access to a message that is communicated from a first node to a second node in a network, the computer-readable medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key ;

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node; and

wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes:

the message to be recovered from the encoded message by

retrieving the key, and

decoding the encoded message using the key, and

the recovered message to be provided from the third node to the second node.

38. (NOT AMENDED) The computer-readable medium as recited in Claim 37, wherein the receiving, at the third node, of the encoded message and the instructions for retrieving the key, further causes the key to be deleted from the third node after the encoded message is decoded.

39. (NOT AMENDED) The computer-readable medium as recited in Claim 37, wherein the set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key comprises an HTML document.

40. (NOT AMENDED) The computer-readable medium as recited in Claim 39, wherein the HTML document comprises an HTML form with fields containing the encoded message and key address data, a submit button to submit the form to the third node, and JavaScript to automatically submit the form to the third node.

41. (NOT AMENDED) The computer-readable medium as recited in Claim 39, wherein the HTML document comprises a set of associated URLs embedded in multiple <img>, <ilayer>, <applet>, or <iframe> elements, wherein each URL contains fragments of the encoded message and key address data as URL query parameters, and wherein each URL specifies the location of the third node.

42. (NOT AMENDED) The computer-readable medium as recited in Claim 41, wherein the URL query parameters also contain control information, which specifies the order and number of message fragments, and enables the third node to reconstruct the complete message.

43. (NOT AMENDED) A computer system for controlling access to a message that is communicated from a first node to a second node in a network, the computer system comprising:

one or more processors; and

a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the one or more processors, causes the one or more processors to perform the steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key;

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node; and

wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes:

the message to be recovered from the encoded message by

retrieving the key, and

decoding the encoded message using the key, and

the recovered message to be provided from the third node to the second node.

44. (NOT AMENDED) The computer system as recited in Claim 43, wherein the receiving, at the third node, of the encoded message and the instructions for retrieving

the key, further causes the key to be deleted from the third node after they encoded message is decoded.

45. (NOT AMENDED) The computer system as recited in Claim 43, wherein the set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key comprises an HTML document.

46. (NOT AMENDED) The computer system as recited in Claim 45, wherein the HTML document comprises an HTML form with fields containing the encoded message and key address data, a submit button to submit the form to the third node, and JavaScript to automatically submit the form to the third node.

47. (NOT AMENDED) The computer system as recited in Claim 45, wherein the HTML document comprises a set of associated URLs embedded in multiple <img>, <ilayer>, <applet>, or <iframe> elements, wherein each URL contains fragments of the encoded message and key address data as URL query parameters, and wherein each URL specifies the location of the third node.

48. (NOT AMENDED) The computer system as recited in Claim 47, wherein the URL query parameters also contain control information, which specifies the order and number of message fragments, and enables the third node to reconstruct the complete message.

49. (ONCE AMENDED) A method for exchanging data between nodes in a network, the method comprising the computer-implemented steps of:

splitting the data into two or more data fragments;

embedding control information and each data fragment from the two or more data fragments in a URL;

[embedding, in one or more associated URLs, data and control information; and]

providing the [set of one or more associated] URLs from a source node to a destination node; and

wherein the two or more data fragments and control information may be extracted from the [set of one or more associated] URLs at the destination node.

50. (ONCE AMENDED) The method as recited in Claim 49, wherein the [set of one or more associated] URLs [is] are provided from the source node to the destination node using the HTTP protocol.

51. (ONCE AMENDED) The method as recited in Claim 50, wherein the [set of one or more associated] URLs [is] are contained within an HTML document.

52. (ONCE AMENDED) The method as recited in Claim 51, wherein each URL [from the set of one or more associated URLs,] contained within the HTML document, is embedded in an <img>, <ilayer>, <applet>, or <iframe> element, contains fragments of the data as URL query parameters, and specifies a location of the destination node.

53. (NOT AMENDED) The method as recited in Claim 52, wherein the URL query parameters also contain control information, which specifies an order and number of data fragments to enable the data to be reconstructed at the destination node.

54. (ONCE AMENDED) The method as recited in Claim 53, wherein:

the HTML document is embedded in a registration email received at the source node,
the data fragments embedded in the [one or more associated] URLs [includes] include registration and user information, and
the method further comprises the computer-implemented steps of:
providing the data to the destination node when the registration email is read;
generating an authentication cookie on the source node in response to receiving the registration and user information;
using the authentication cookie to authenticate a user at the source node when the source node makes subsequent client requests to the destination node.

55. (ONCE AMENDED) A computer-readable medium for exchanging data between nodes in a network, the computer-readable medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:
splitting the data into two or more data fragments;
embedding control information and each data fragment from the two or more data fragments in a URL;
[embedding, in one or more associated URLs, data and control information; and]
providing the [set of one or more associated] URLs from a source node to a destination node;
wherein the two or more data fragments and control information may be extracted from the [set of one or more associated] URLs at the destination node.

56. (ONCE AMENDED) The computer-readable medium as recited in Claim 55, wherein the [set of one or more associated] URLs [is] are provided from the source node to the destination node using the HTTP protocol.

57. (ONCE AMENDED) The computer-readable medium as recited in Claim 56, wherein the [set of one or more associated] URLs [is] are contained within an HTML document.

58. (ONCE AMENDED) The computer-readable medium as recited in Claim 57, wherein each URL [from the set of one or more associated URLs,] contained within the HTML document, is embedded in an <img>, <ilayer>, <applet>, or <iframe> element, contains fragments of the data as URL query parameters, and specifies a location of the destination node.

59. (NOT AMENDED) The computer-readable medium as recited in Claim 58, wherein the URL query parameters also contain control information, which specifies an order and number of data fragments to enable the data to be reconstructed at the destination node.

60. (ONCE AMENDED) The computer-readable medium as recited in Claim 59, wherein:

the HTML document is embedded in a registration email received at the source node,

the data fragments embedded in the [one or more associated] URLs [includes] include registration and user information, and

the computer-readable medium further comprises one or more additional sequences of one or more instructions which, when executed by the one or more processors,

causes the one or more processors to perform the computer-implemented steps of:

providing the data to the destination node when the registration email is read;

generating an authentication cookie on the source node in response to receiving the registration and user information;

using the authentication cookie to authenticate a user at the source node when the source node makes subsequent client requests to the destination node.

61. (ONCE AMENDED) A computer system comprising:

one or more processors; and

a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

splitting the data into two or more data fragments;

embedding control information and each data fragment from the two or more data fragments in a URL;

[embedding, in one or more associated URLs, data and control information; and]

providing the [set of one or more associated] URLs from a source node to a destination node;

wherein the two or more data fragments and control information may be extracted from the [set of one or more associated] URLs at the destination node.

62. (ONCE AMENDED) The computer system as recited in Claim 61, wherein the [set of one or more associated] URLs [is] are provided from the source node to the destination node using the HTTP protocol.

63. (ONCE AMENDED) The computer system as recited in Claim 62, wherein the [set of one or more associated] URLs [is] are contained within an HTML document.

64. (ONCE AMENDED) The computer system as recited in Claim 63, wherein each URL [from the set of one or more associated URLs,] contained within the HTML document, is embedded in an <img>, <ilayer>, <applet>, or <iframe> element, contains fragments of the data as URL query parameters, and specifies a location of the destination node.

65. (NOT AMENDED) The computer system as recited in Claim 64, wherein the URL query parameters also contain control information, which specifies an order and number of data fragments to enable the data to be reconstructed at the destination node.

66. (ONCE AMENDED) The computer system as recited in Claim 65, wherein:

the HTML document is embedded in a registration email received at the source node,

the data fragments embedded in the [one or more associated] URLs [includes] include registration and user information, and

the memory further comprises one or more additional sequences of one or more instructions which, when executed by the one or more processors, causes the one or more processors to perform the computer-implemented steps of:

providing the data to the destination node when the registration email is read;

generating an authentication cookie on the source node in response to receiving the registration and user information;

using the authentication cookie to authenticate a user at the source node when the source node makes subsequent client requests to the destination node.